The Implication of the Security Key Exchange during Mobile IPv6 Smooth Handoff

Tin-Yu Wu, Ting-Shi Tsai and Han-Chieh Chao
Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, Republic of China
E-mail: {tyw, hcc}@mail.ndhu.edu.tw

Abstract—**The number of action devices is currently increasing. If the trade environments are not safe, both the development and the progress of electronic trade will be affected. As well as security issues, the handoff procedure incurs long latency and packet loss. Smooth handoff can not only lower the packet loss but also reduce the level of the out-of-sequence packets. So far, very little attention has been given to the Internet Key Exchange for encryption in Mobile network. This study examines Internet Key Exchange in smooth handoff for Mobile IPv6 network, and compares the proposed method with the classic smooth handoff technologies. It shows that the proposed solution is more efficient in Mobile IPv6 networks.**

Keywords —**Mobile IPv6, Key Exchange, Smooth handoff**

1. Introduction

Since the air is the transmission medium in the wireless communication environment, the low bandwidth, high error rate and other factors often lead to the packet retransmission in the wireless network. In addition to the low transmission rate which is a feature characteristic of wireless internet transmission networks, the packet loss prevention is also a very important goal. The mechanism cannot be used totally in the wireless network environment, more questions need to be considered about how it could be employed under the wireless network environment.

This investigation discusses the mechanism that Internet key exchange in smooth handoff for IPv6 wireless network. After packets in the cache are forwarded to the mobile node, the Internet key exchange is executed. When the mobile node hands off, it needs to do the whole handoff processes and confirms the passing-on movements of the address (Care-of Address) that is RR (Return Routability) Procedure. Under the wireless network environment in IKE, mobile node needs to exchange some information. It could finish the movements along with the Internet key exchange by using RR Procedure to confirm CoA (Care-of Address), and let the correspondent node so that the mobile node confirm this address. When the RR procedure is executed, IKE is also finished. The whole procedure can quickly set up a secure tunnel between the correspondent node and the mobile node. It can reduce the time to exchange the Internet key.

The rest of this paper is organized as follows. Section 2 introduces the motivation and the related works. Section 3 is about the proposed methodology and simulation model. Section 4 presents the simulation results. Conclusions are finally drawn in Section 5.

2. Motivation

A. Return routability procedure and route optimization

Route optimization mechanism [1][2] is mainly used to alleviate the triangular route problem. It makes correspondent nodes send packets to mobile node directly without passing through Home Agent, as indicated in Figure 1. The route optimization mechanism is better than triangular route in both time delay and resource consumption. It also enhances the performance of the original Mobile IP.

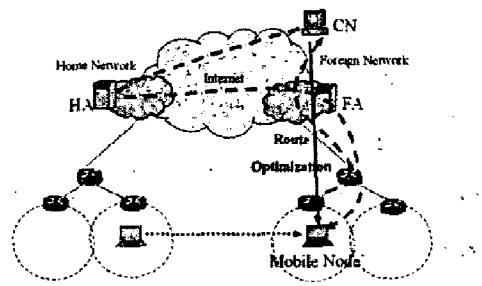

Figure 1. Triangle Routing

Route optimization is introduced just only as a supplementary method in Mobile IPv4 because of the security issues caused by existing firewalls, for example, ingress filtering. When using route optimization mechanism, correspondent node has to know the current CoA of the mobile node. If the notification from the CoA of the mobile node to the correspondent node is not adapted in a secure authentication mechanism, the route optimization mechanism is vulnerable to DoS (Denial-of-Service) attacks. The challenge of developing the authentication mechanism is the key transmission between the mobile node and the correspondent node. If both ends can dynamically retrieve the key securely, the authentication mechanism will not only work as intended but also ensure the security of the route optimization mechanism.

RR Procedure is employed for the correspondent node to discover the CoA of the mobile node, as illustrated in Figure 2. With this procedure, correspondent node can accept CoA without passing through the home agent during binding updates between the correspondent node and the mobile node.

The first stage of the RR Procedure is that the mobile node sends two messages simultaneously to the correspondent node: Home Test Init (HoTI) and Care of Test Init (CoTI). HoTI is sent to correspondent node through the Home Agent, and CoTI is transmitted there directly.

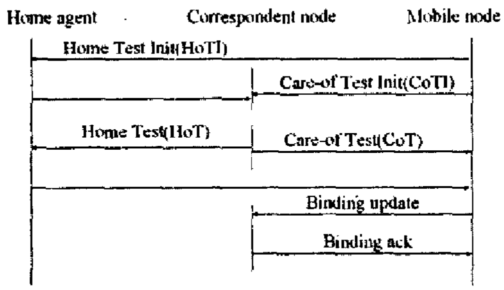

Figure 2. Return Routability Procedure

When the correspondent node receives the HoTI and CoTI message, it responds with two messages: the Home Test (HoT) and the Care-of Test (CoT). HoT is also back to mobile node through home agent, and CoT is directly sent back to the mobile node. The RR procedure is completed after these steps.

Importantly, when the correspondent node receives the HoTI and CoTI messages, it first generates a home keyen token and applies the current nonce index as the home nonce index, and second creates a care-of nonce that employs the current nonce index as the care-of nonce index. The nonce index passes on the address to discern according to the primitive address of mobile node carried in the information makes HoTI and CoTI information, creates HoT information and CoT information and then sends them out, making the mobile node produce the key:

Home keygen token = First(64, HMAC_SHA1(Kcn, (home address | nonce |0)))

Care-of keygen token =First(64, HMAC_SHA1(Kcn, (care-of address | nonce |1)))

Kbm = SHA1 (home keygen token | care-of keygen token)

Then the mobile node and correspondent node obtain the communication key Kbm, which is used to ensure the authorization of subsequent Binding Updates to initiate the link renewal process. It is obvious that the authentication is protected in the route optimization mechanism.

B. Classic smooth handoff

Handoff occurs when a mobile node moves from one subnet to another. The new access router takes over the role of serving the mobile node from old access router. During the handoff process, some packets are loss. It's because the delay which occurs when a mobile node changes access router. During this process, the correspondent node continues sending packets to the mobile node, and these packets are lost during handoff.

During smooth handoff, packets are held in the buffer to reduce the probability of losing packets [3][4], but after, the handoff correspondent begins to transmit data to the new care-of address. At this time, packets are out-of-sequence as in Figure 3.

By Figure 4, where each time expresses an occurred event:

- Tin: Handoff initiation
- Ts-MN-CN: MN sends a Binding Update to the CN
- Tr-CN-MN: CN sends a Binding ACK to the MN
- Tf-CN-AR2: CN forwards the first packet to AR2
- Tr-MN-AR1: MN sends request forwarding to the AR1
- Tf-AR1-MN: AR1 forward MN's buffered packets to AR2
- Ta-CN-MN: Arriving of the first packets from the CN to the MN through AR2
- Ta-AR1-MN: Arriving of the last packet forwarded by the AR1 to the MN

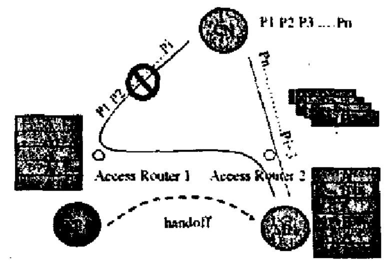

Figure 3. Out-of-sequence in Classic Smooth handoff

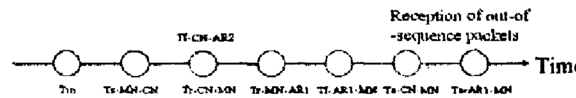

Figure 4. Classic Smooth handoff time slot

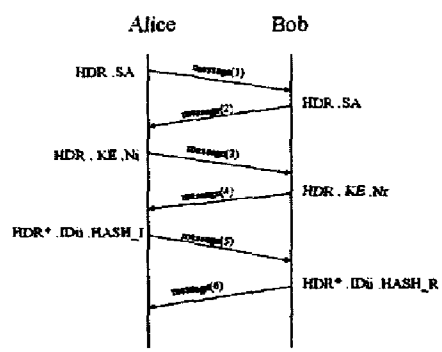

Figure 5. Pre-shared key main mode

C.IKE Overview

IPv6 using IPsec to protect communication hosts. A full IPsec includes the key to exchange and also other mechanism used in IP AH and IP ESP [5][6][7]; IKE is the IPsec key which exchanges management protocol. However, to implement IKE, it must support at least the User Datagram Protocol (UDP) at port 500. IKE establishes a secure framework for the distribution of public keys. Additionally, IKE defines how those keys will be created. The main mode [8] of IKE uses six messages to finish the negotiation and authentication of key, as indicated in Figure 5.

3. Proposed approach

The increasing popularity of wireless networking means that the network security becomes more important. When a terminal device moves to a new wireless area, Internet key exchange must be assured to be effective, and each packet is transmitted smoothly from source to destination without any lost during transmission, and every packet uses the correct key to encryption and decrypt. This session discusses the Internet key exchange in enhanced smooth handoff with Security Consideration for mobile IPv6 network.

A. Enhanced secure key exchange

This study discusses the method of key exchange to merge the main modes of IKE and RR during binding procedure in mobile IPv6. According to the RFC [1] of Mobile IPv6 handoff mechanism, RR is executed in every handoff. The RR procedure ensures CoA for the correspondent node. This work uses the main mode of IKE and RR to build the secure key.

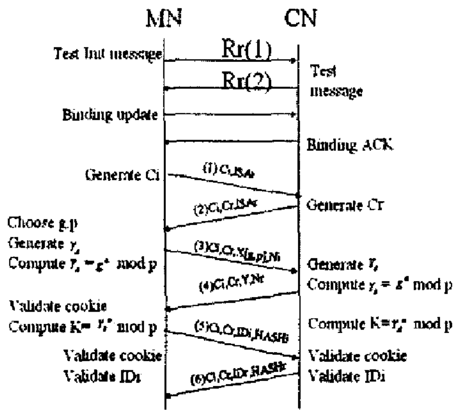

Figure 6. Complete message

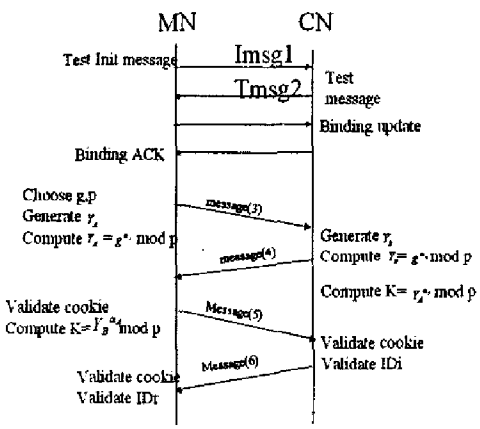

Figure 7. Integrated message

The RR procedure ensures that the correspondent node can confirm the mobile node's new CoA. It also integrates the RR procedure of mobile IPv6 and IKE exchange key at the first stage. The procedure also uses the buffer characteristic of smooth handoff to make users unaware of packet loss. A handoff message is combined with Pre-shared key main mode. This is shown to have not only RR message, Binding Update message and Binding Acknowledge message [1][5], but also key exchange message, such as Figure 6.

In the Pre-shared key main mode, it has some message that is the same as RR. So some messages can be decreased to become more efficient as shown in Figure 7.

The network security can be enhanced if the key can be exchanged during handoff. We combine Return Rout ability, which is combined with IKE to reduce key exchange time as expressed in the following equation.

$$Im + Tm + Tbu + Tba + Msg1 + Msg2 + Msg3 + Msg4 + Msg5 + Msg6 > Imsg1 + Tmsg2 + Tbu + Tba + Msg3 + Msg4 + Msg5 + Msg6$$

B. Enhanced Smooth Handoff with Security Consideration

Although the classic smooth handoff can reduce the packet loss, it leads to out-of-sequence packets. In [7][11], its technique anticipates the forwarding of MN's packets from the current foreign agent to the new one, while the mobile node initiates its handoff in mobile IPv4 network. The level of out-of-sequence packets can be reduced. Reference [8] is about some cases of smooth handoff in mobile IPv6 network. It is proposed to employ the prioritized queuing for the stray packets in a router during the smooth handoff, which can significantly reduce the transient period. This study proposes a new enhanced smooth handoff incorporating security considerations. This point is that when a mobile node sends a request forwarding to AR1and tell that it is forwarding packets to AR2 before binding procedure. This technique can reduce the level of stray packets. Moreover, most kinds of smooth handoff do not consider security; therefore, the proposed scheme can enhance smooth handoff with security consideration. Mechanism can solve both the security problem and the out-of sequence packet problem.

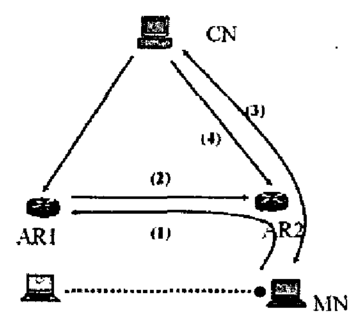

Figure 8. Enhanced Smooth Handoff with Security Consideration

Figure 8 illustrates the proposed enhanced smooth handoff with security consideration after MN obtains a new CoA. The process is as follows:

(1) The MN sends a request forwarding to AR1.
(2) AR1 starts to forward MN's packets to AR2. AR2 stores these packets.
(3) The MN runs binding update and Internet key exchange.
(4) The CN starts to send message to AR2.

The proposed algorithm is based on the classic smooth handoff and undertakes Internet key exchange after the binding procedure. Since the duration of the key replacement is not firmly decided, we suggest that Handoff and exchange key method are processed in simultaneous time.

4. Simulation results

Scenario 1: Non-buffer situation

In reference [10], there aren't any buffer situation results in the packet loss. This study simulates actions to show the conditions for packet lost during handoff. The experiment assumes that the correspondent node has sent UDP packets to the mobile node and it does not consider handoff as that is taken places bellowing the third layer of the OSI model. Even if the conditions are optimal, it has some difference of time. Then packet loss may result during handoff as depicts in Figure 9.

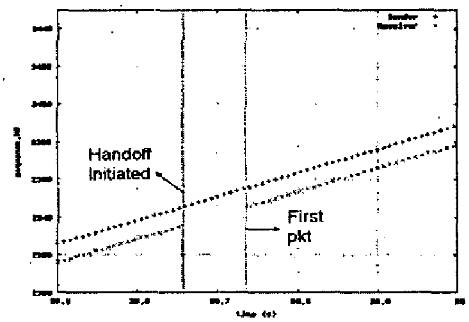

Figure 9. Diagram of UDP sequence during handoff (Non-Forward)

Scenario 2: Classic Smooth handoff Mechanism

According to the reference [1][2][9], Mobile IPv4 operation and Mobile IPv6 operation are virtually identical. Handoff is assumed to be already completed and AR1 starts to forward packets to AR2. At this time, our-of-sequence packets should result. Figure 10 explains the timeline of events while a handoff is undertaken.

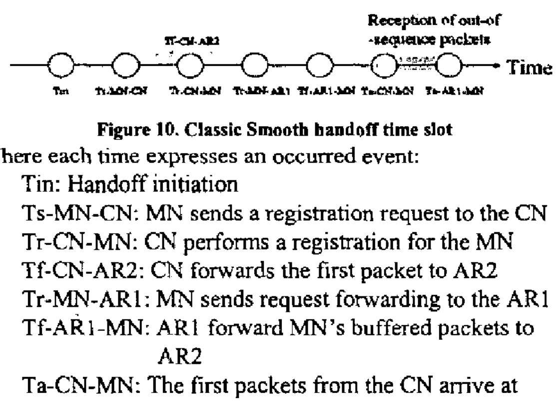

Figure 10. Classic Smooth handoff time slot

Where each time expresses an occurred event:

- Tin: Handoff initiation
- Ts-MN-CN: MN sends a registration request to the CN
- Tr-CN-MN: CN performs a registration for the MN
- Tf-CN-AR2: CN forwards the first packet to AR2
- Tr-MN-AR1: MN sends request forwarding to the AR1
- Tf-AR1-MN: AR1 forward MN's buffered packets to AR2
- Ta-CN-MN: The first packets from the CN arrive at MN through AR2
- Ta-AR1-MN: The last packet forwarded by the AR1arrive at the MN

Scenario 3: Predicted Smooth handoff Mechanism [9].

According to reference [9], the technique anticipates the forwarding of packets from the current router (AR1) to the new one (AR2) while the mobile node initiates its handoff. Although this method can reduce the level of out-of-sequence packets, it cannot be considered as a secure problem; on the contrary, it may cause more danger. Figure11 explains the time of events while executing a handoff.

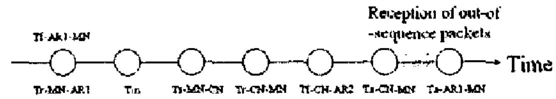

Figure 11. predicted Smooth handoff time slot.

Where each time expresses an occurred event:

- Tr-MN-AR1: MN sends request forwarding to the AR1
- Tf-AR1-MN: AR1 forward MN's buffered packets to AR2
- Tin: Handoff initiation
- Ts-MN-CN: MN sends a registration request to the CN
- Tr-CN-MN: CN undertakes a registration for the MN
- Tf-CN-AR2: CN forwards the first packet to AR2
- Ta-CN-MN: The first packets from the CN arrive at MN through AR2
- Ta-AR1-MN: The last packets forwarded by the AR1 arrive at the MN

Scenario 3: Predicted Smooth Handoff Mechanism [5]

According to the purpose from reference [5], its technique anticipates the forwarding of packets from the current router(AR1) to the new one(AR2) while the mobile node initiates its handoff. Although this method can reduce packet out-of-sequence but it can't consider security problem. It may cause more danger. Figure 4-12 explains the time of events while doing a handoff.

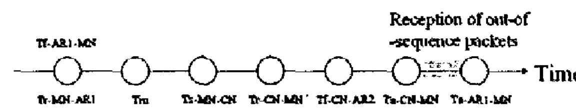

Figure.4-12 predicted Smooth handoff time slot

Where each time expresses an occurred event:

- Tr-MN-AR1:MN sends request forwarding to the AR1
- Tf-AR1-MN:AR1 forward MN's buffered packets to AR2
- Tin: Handoff initiation
- Ts-MN-CN:MN sends a registration request to the CN
- Tr-CN-MN:CN does a registration for the MN
- Tf-CN-AR2:CN forwards the first packet to AR2
- Ta-CN-MN: Arriving of the first packets from the CN to the MN through AR2
- Ta-AR1-MN:Arriving of the last packet forwarded by the AR1 to the MN

Scenario 4: Enhanced Smooth Handoff with Security Consideration Mechanism

The correspondent node is assumed to transmit packets to mobile node in mobile IPv6. When the mobile node leaves the old subnet, it needs to send out a binding update to both home agent and correspondent node. Therefore, it causes binding time during each handoff. Figure12 explains the time of events while doing a handoff.

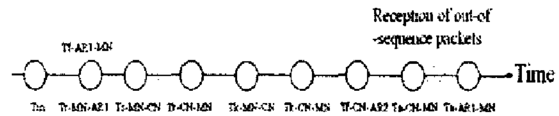

Figure12. Enhanced Smooth Handoff with Security Consideration time slot

Where each time expresses an occurred event:

- Tin: Handoff initiation
- Tr-MN-AR1: MN sends request forwarding to the AR1
- Tf-AR1-MN: AR1 forward MN's buffered packets to AR2
- Ts-MN-CN: MN sends a binding update message to the CN
- Tr-CN-MN: CN sends a binding acknowledgement message to the MN
- Tk-MN-CN: MN sends a key message to the CN
- Tk-CN-MN: CN replies with a key message for the MN
- Tf-CN-AR2: CN forwards the first packet to AR2
- Ta-CN-MN: The first packets from the CN arrive at the MN through AR2
- Ta-AR1-MN: The last packets forwarded by the AR1 arrive at the MN

Figure13 and 14 shows simulation for mobile nodes which perform handoff from one subnet to another, and it is based on scenario 2 and 4 respectively. In these figures, the X-axis denotes time, and Y-axis is the sequence number of each packet. The symbol "+" represents the time when the sender sends each packet, and the symbol "x" represents the time when the receiver receives each packet.

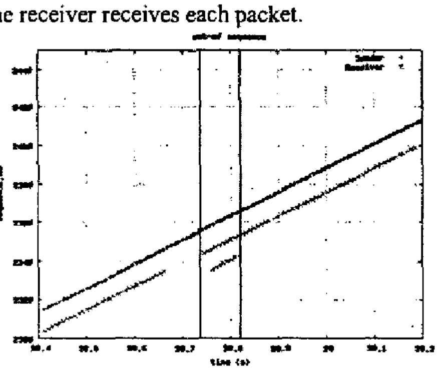

Figure 13. Classic Smooth Handoff out-of sequence

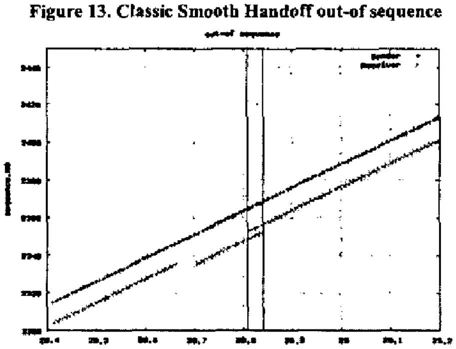

Figure 14. Out-of-sequence of Enhanced Smooth Handoff with Security Consideration

Figure 13 shows a simulation of the classic smooth handoff. A mobile node has a span of time during not receiving packets during handoff, and the figure shows that if the sender sends packets to the receiver without interruption, then the receiver has some latency until it restores its ability to receive packets. Since the new access router can receive the packets from the corresponding node and the old access router at the same time, an out-of-sequence time may be resulted.

Figure 14 shows the proposed Enhanced Smooth Handoff with Security Consideration. A request of old access forwarding packets to the new access router is anticipated before executing the binding update, to further reduce the out-of-sequence time beyond the classic smooth handoff.

Besides simulating the proposed solution – scenario 4 and classic smooth handoff - scenario 2, we will prove that the proposed solution can reduce the time of our-of-sequence packets.

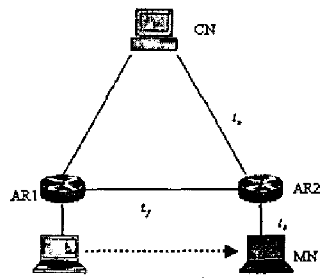

Figure 15. Inference topology

According to the Figure 15, we define some variable parameter:

t_{over} : The time that the remaining packets after binding update (including key exchange) need to spend.

t_{old} : The time until the last packet of old stream packet arrives from CN to AR2.

t_{new} : Defined as the time until the first packet of new stream arrives from CN to AR2

t_{out} :The out-of-sequence time

$t_{out} = t_{old} - t_{new}$

t_h : Handoff time

t_u :Including binding procedure time, RR procedure and internet key exchange time.

t_k : MN and CN key exchange time

t_f : Time between AR1 and AR2

t_n : Time between CN and AR2

t_b : Time between AR2 and MN

k: packets from other CN transmit to AR1

Δp : the number of packets between the HA and the AR1 when MN initiates the handoff process.

D1: the transmission rate from CN to AR1.

D2: the transmission rate from AR1 to AR2.

1. According to scenario 2:

$$\begin{cases} t_{new1} = t_h + t_u + t_n \\ t_{old1} = t_h + t_u + t_b + t_f + t_{over1} \\ t_{over1} = \left((t_h + t_u) * D1 + \Delta p + k \right) / D2 \end{cases}$$

$$\begin{aligned} & t_{old1} \\ & = t_h + t_u + t_b + t_f + t_{over1} \\ & = t_h + t_u + t_b + t_f + \left(\left((t_h + t_u) * D1 + \Delta p + k \right) / D2 \right) \\ & = \left(\left((t_h + t_u) * D1 + \Delta p + k \right) / D2 \right) + t_h + t_u + t_b + t_f \end{aligned}$$

$$\begin{aligned} & t_{out1} \\ & = t_{old1} - t_{new1} \\ & = \left(\left(\left((t_h + t_u) * D1 + \Delta p + k \right) / D2 \right) + t_h + t_u + t_b + t_f \right) - (t_h + t_u + t_n) \\ & = \left((t_h + t_u) * D1 + \Delta p + k \right) / D2 + t_b + t_f - t_n \end{aligned}$$

2. According to scenario 4:

Since some packets of AR1 buffer have already been forwarded from AR1 to AR2 before the binding update has finished, t_{over} must subtract some packets.

$$\begin{cases} t_{new2} = t_h + t_b + t_f + t_u + t_k + t_n \\ t_{old2} = t_h + t_b + t_f + t_u + t_k + t_{over2} \\ t_{over2} = \left(\left((t_h + t_b + t_f + t_u + t_k) * D1 + \Delta p + k \right) - (t_u + t_k) * D2 \right) / D2 \end{cases}$$

$$\begin{aligned} & t_{old2} \\ & = t_h + t_b + t_f + t_u + t_k + t_{over2} \\ & = t_h + t_u + t_k + t_b + t_f \\ & + \left(\left(\left((t_h + t_b + t_f + t_u + t_k) * D1 + \Delta p + k \right) - (t_u + t_k) * D2 \right) / D2 \right) \\ & = t_h + t_u + t_k + t_b + t_f \\ & + \left(\left((t_h + t_b + t_f + t_u + t_k) \bullet D1 + \Delta p + k \right) / D2 - t_u - t_k \right) \\ & = \left((t_h + t_b + t_f + t_u + t_k) * D1 + \Delta p + k \right) / D2 \\ & + t_h + t_b + t_f \end{aligned}$$

$$\begin{aligned} & t_{out2} \\ & = t_{old2} - t_{new2} \\ & = \left(\left((t_h + t_b + t_f + t_u + t_k) * D1 + \Delta p + k \right) / D2 + t_h + t_b + t_f \right) \\ & - (t_h + t_b + t_f + t_u + t_k + t_n) \\ & = \left(\left((t_h + t_b + t_f + t_u) * D1 + \Delta p + k \right) / D2 + t_h + t_b + t_f \right) \\ & + t_k \bullet (D1/D2) - (t_h + t_b + t_f + t_u + t_k + t_n) \\ & = \left(\left((t_h + t_b + t_f + t_u) * D1 + \Delta p + k \right) / D2 - t_n \right) \\ & + t_k * (D1/D2 - 1) - t_u \\ & = \left(\left((t_h + t_u) * D1 + \Delta p + k \right) / D2 - t_n \right) \\ & + \left((t_b + t_f) * D1 / D2 \right) \\ & + t_k * (D1/D2 - 1) - t_u \end{aligned}$$

AR1 and AR2 are usually nearer than AR1 and CN. In theory, transmission rate should be represented by D2>=D1. From the above inference, the conclusion is that our solution can reduce more time of our-of-sequence packets than classic smooth handoff.

5. Conclusion

This paper proposes an enhanced smooth handoff with security consideration for Mobile IPv6. The mobile node sends a request forwarding to the old access router before the mobile node begins to execute the binding update. This work also discusses the key exchange method to combine the main mode of IKE and finish handoff during Return Rout ability Procedure, and key exchange for Mobile IPv6.

The method we proposed can not only reduce the incidence of out-of-sequence packets but also execute Internet key exchange in smooth handoff. What's more, it establishes a better environment for mobile network.

6. Acknowledgement

The authors would like to thank R. C. Wang for helpful discussion and the National Science Council of the Republic of China, Taiwan for financially supporting this research under Contract No. NSC 92-2219-E-259-002-.

7. References

[1] D.Johnson ; C.Pekins and j,Arkko. "Mobility support in IPv6" RFC 3775, Ineternet Engineering Task Force, June, 2004

[2] Perkins, C.E and Wang, K.Y, "Optimized Smooth Handoffs in Mobile IP", Processdings of the Fourth IEEE Symposium on Computers and Communications, July ,1999.

[3] Tandjaoui, D.; Badache, N.; Bettahar,H.; Bouabdallah,A.; Seba,H.;" Performance enhancement of smooth handoff in mobile IP by reducing packets disorder" Computers and Communication, 2003. (ISCC 2003). Proceedings. Eighth IEEE International Symposium on , 2003

[4] Dongwook Lee and JongWon Kim Networked Media Lab, "Analysis and Reduction of Transient Time Periods for Smooth Handoff Packets in Mobile IPv6 Networks" ,Department of Inforamation and Communications, Kwang-ju Institute of Science and Technology, Gwagnju,Korea

[5] Principles and Practice –Second Edition "CRYPTOGRAPHY AND NETWORK SECURITY"

[6] Perlman, R.; Kaufman, C ; "Key exchange in IPSec: analysis of IKE" Internet Computing, IEEE , Nov.-Dec, 2000

[7] Arkko,J.,v.Devarapalli,and F.Dupont, "Using IPsec to protect Mobile Ipv6 Signaling between Mobile Nodes and Home Agent, RFC 3776",work in progress, June,2004

[8] D. Harkins and D. Carrel, "The Internet Key Exchange Protocol (IKE)," IETF RFC 2409, Nov. 1998; available at http://www.ietf.org/rfc/rfc2409.txt.

[9] Hesham Soliman. "Mobile IPv6 Mobility in Wireless Internet" First printing,, April, 2004

[10]Hsieh,Ming-Fu; Yeali S.Sun; "Neighbor-Cooperated Multicast for seamless handoff in Mobile IPv6" ,July,2002

[11]Han-Chieh Chao; Ching-Yang Huang, "Micro-mobility mechanism for smooth handoffs in an integrated ad-hoc and cellular IPv6 network under high-speed movement",IEEE Transactions, Nov, 2003